PATENT APPLICATION
Attorney Docket No. JP919990266US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Jing Min XU et al.	Examiner: Leslie WONG
Serial No: 09/754,813	Art Unit: 2164
Filed: January 4, 2001	
For: A METHOD AND A SYSTEM FOR CERTIFICATE REVOCATION LIST CONSOLIDATION AND ACCESS	

REVISED APPEAL BRIEF

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This revised Appeal Brief is submitted in response to the Notification of Non-Compliant Appeal Brief dated December 31, 2007 setting a one-month shortened statutory period of brief filing expiring January 31, 2008.

No fee is believed due with this brief, however, should a fee be required please charge Deposit Account 50-0510.

Real Party in Interest

The real party in interest is International Business Machines Corporation, as evidenced by the assignment set forth at Reel 011786, Frame 0585.

Related Appeals and Interferences

None.

Status of Claims

Claims 1-15 and 17-21 are pending in the instant application, with claims 1, 11, and 18 being independent claims. Claim 16 is cancelled.

Claims 1-15 and 17-21 stand finally rejected by the Examiner as noted in the Final Office Action dated May 31, 2005 ("FOA"). The rejection of claims 1-15 and 17-21 is appealed.

The table below summarizes the status of the claims.

Claim(s)	Status	Appealed
1	Amended	Yes
2-4	Original	Yes
5	Amended	Yes
6-8	Original	Yes
9-11	Amended	Yes
12	Original	Yes
13-14	Amended	Yes
15	Original	Yes
16	Canceled	No
17	Original	Yes
18	Amended	Yes
19-21	Original	Yes

Status of Amendments

No amendments to the claims were made after the final rejection.

Summary of the Claimed Subject Matter

The present invention relates to digital signature certificates and certificate revocation lists. App., pg. 1, ln. 4-6. Digital signature certificates are used in electronic commerce to authenticate subscribers (e.g., merchants) that rely on digital signatures. Digital signature certificates are issued by several trusted third parties known as certificate authorities (CAs). App., pg. 2, ln. 1-10.

Sometimes a CA revokes a certificate, and the revoked certificate is listed in a certificate revocation list (CRL). App., pg. 3, ln. 19-21. Different CAs may use a different CRL distribution mechanisms, and a party checking CRLs needs to know each distribution mechanism. App., pg. 4, ln. 14-18. Furthermore, some CAs may change their CRL distribution mechanisms from time to time, and this may impose significant modification to the way applications can access their CRL. App., pg. 4, ln. 18-21.

With this brief background, one aspect of the present invention, as recited in claim 1, is a system that includes a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and different CAs may use different CRL distribution mechanisms. App., Fig. 1. For different CRL distribution methods, different CRL retrieval agents are used to periodically retrieve CRLs from different CAs and consolidate them into a central CRL database. App., pg. 11, ln. 11-16. These agents are configured to reside at the central database, run periodically to retrieve CRLs from designated servers, and update the central database accordingly. App., pg. 12, ln. 3-6.

For example, agents such as an LDAP Retriever, HTTP Retriever, RFC1424 Requester, RFC1424 Receiver and HttpReceiver are described in the specification of the pending application. App., pg. 16, ln. 5-7. Each agent is designed to conform to a

particular distribution mechanism. Thus, the present invention enables an electronic commerce application to have easier, faster and less costly access to CRLs in a central location. App., pg. 12, ln. 7-16.

The CRL databases are configured to store at least one individually identifiable revoked digital certificate. App., pg. 8, ln. 16-18. Additionally, the system includes a CRL access user interface which provides a uniform set of Application Program Interfaces for users accessing the CRLs in the CRL database. App., pg. 12, ln. 13-16. Thus, the system enables consolidation and access of the certificate revocation lists (CRLs) from the plurality of certificate authorities (CAs). App., pg. 21, ln. 9-18 and Fig. 8.

Similarly, the invention may be embodied as a method for certificate revocation list consolidation and access in a secure network, such as recited in claim 11 of the present application. App., pg. 21, ln. 19 - pg. 22, ln. 2 and Fig. 8. The method may be employed in systems with a plurality of certificate authorities (CAs) that maintain and distribute the digital certificates revoked by themselves in the form of CRLs, and different CAs may use different CRL distribution mechanisms. App., pg. 11, ln. 11-16, Fig. 1.

A retrieving operation periodically retrieves CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs. App., pg. 18, ln. 2-4. The CRLs are consolidated and stored into a plurality of CRL databases. App., pg. 21, ln. 27-31 and Fig. 8, item 801 and 802. The consolidated CRLs include at least one individually identifiable revoked digital certificate. App., pg. 8, ln. 16-18. An accessing operation accesses the CRLs from the CRL databases by a uniform set of Application Program Interfaces. App., pg. 12, ln. 13-16, Fig. 8, item 804.

Claim 14 recites an article of manufacture including a computer usable medium having computer readable program code means

embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in the article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11. App., pg. 22, ln. 14-25.

Claim 15 recites a computer program product including a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in the computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11. App., pg. 22, ln. 14-25.

At claim 18, the method recites employing a secure network implemented by digital certificates for certificate revocation list (CRL) consolidation and access, with a plurality of certificate authorities (CAs) maintaining and distributing the digital certificates revoked by themselves in the form of CRLs, wherein different CAs may use different CRL distribution mechanisms. App., pg. 11, ln. 11-16, Fig. 1.

The method includes creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, the retrieval agents configured to periodically retrieve CRLs at time intervals from the different CAs and to consolidate the CRLs from multiple CAs; storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate; and accessing the CRLs form the CRL databases by a uniform set of Application Program Interfaces. App., pg. 21, ln. 27 - pg. 22, ln. 2, Fig. 8, items 801 to 804.

Claim 19 recites a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation

list (CRL) consolidation and access, the method steps comprising the steps of claim 18. App., pg. 22, ln. 14-25.

Claim 20 recites an article of manufacture including a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in the article of manufacture including computer readable program code means for causing a computer to effect the steps of claim 18. App., pg. 22, ln. 14-25.

Claim 21 recites a computer program product including a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in the computer program product including computer readable program code means for causing a computer to effect the steps of claim 18. App., pg. 22, ln. 14-25.

Grounds for Rejection to be Reviewed on Appeal

I. Claims 1, 4, 6, 7, 10, 11, 13-15 and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US 6,442,689) in view of Curry (US 6,128,740) and further in view of Ng (US 6,411,956).

II. Claims 2, 8 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry and Ng, and further in view of Ginter (US 6,658,568).

III. Claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry in view of Ng, and further in view of Vesna Hassler, "X.500 and LDAP security: a comparative overview", Network, IEEE, Vol. 13, Issue, pp. 54-64 (Nov.-Dec. 1999) ("Hassler").

IV. Claim 5 was rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry in view of Ng, and further in view of Kaliski, B, "Privacy Enhancement for Internet

Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, pp. 1-8 (Feb. 1993) ("Kaliski").

V. Claim 9 was rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry in view of Ng in view of Ginter, and further in view of Strellis (US 6,304,882).

Argument

I. Claims 1, 4, 6, 7, 10, 11, 13-15 and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US 6,442,689) in view of Curry (US 6,128,740) and further in view of Ng (US 6,411,956)

Claim 1

Claim 1 was rejected as allegedly obvious over U.S. Patent No. 6,442,689 issued to Kocher (herein "Kocher") in view of U.S. Patent No. 6,128,740 issued to Curry et al. (herein "Curry") and in further view of U.S. Patent No. 6,411,956 issued to Ng (herein "Ng"). FOA, pg. 2. A *prima facie* case for obviousness can only be made if the combined reference documents teach or suggest all the claim limitations. MPEP 2143.

Claim 1 recites, in part, "multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs." App., claim 1. The Final Office Action concedes that neither Kocher nor Ng teach such limitations, but alleges Curry discloses the claim element at column 2, lines 26-41. FOA, pg. 3, ln. 1-4. The Appellant respectfully disagrees with the Examiner's interpretation of Curry's teachings.

The citation offered by the Examiner states,

> Conversely, if certificate revocation lists are published too frequently, such as every ten minutes, a significant overhead burden is placed on the certification authority server (manager) which can significantly reduce the efficiency of the overall system particularly where a

> manager may serve hundreds of thousands of clients. Other systems are known which allow a client to cache certificate revocation lists for a period of time to reduce communication overhead with the manager. Some such known security systems for networked computers also segment certificate revocation list in repository memory to allow recordation of both revocation data and the expiry lapse data. However such systems again, typically only utilize certification authorities or managers that collect revoked certificates and queue them to publish them on a periodic basis with other existing revoked certificates. Curry, col. 2, ln. 26-41.

Contrary to the Examiner's assertions, this passage discusses publishing CRLs by CAs, and does not describe retrieval agents configured to periodically retrieve CRLs. The passage mentions systems that allow a client to cache certificate revocation lists for a period of time to reduce communication overhead with the manager, but there is no teaching of multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, as recited in claim 1.

The Examiner states, "Curry teaches utilizing certification authorities or managers collect revoked certificates and queue them to publish them on periodic basis." FOA, pg. 9-10. Again, the Appellant submits that such a statement does not describe retrieval agents configured to periodically retrieve CRLs.

It is therefore respectfully submitted that the cited art does not respond to the limitation of claim 1 requiring multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs.

In proposing to combine Kocher and Curry to account for the multiple CRL retrieval agents arrangement specified in claim 1 and missing in Kocher, the Examiner submits that it would have been obvious to one of ordinary skill in the art "to modify the CRL system of Kocher by incorporating the means of using multiple CRL retrieval agents to periodically retrieve CRLs as disclosed by

Curry." FOA, pg. 3, ln. 4-7. However, as discussed above, this alleged motivation is based on the false premise that such a teaching exists in Curry.

Moreover, obviousness cannot be established by combining prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. In re Fritch, 972 F.2d 1260, 1266, 23 USPQ2d 1780, 1783-84 (Fed. Cir. 1992). The mere fact that the prior art may be modified in the manner suggested by an examiner does not make the modification obvious unless the prior art suggested the desirability of the modification. Id.

In the present case, the advantage alleged by the Examiner to justify the proposed combination of Kocher and Curry does not stand up to close scrutiny. More particularly, the Examiner has not explained, and it is not evident, why a person of ordinary skill in the art would have found it obvious to reconstruct the Kocher system for creating digitally-signed lists to include the certificate revocation publishing methods taught by Curry. In this light, it is apparent that the only suggestion for combining Kocher and Curry in the manner advanced by the Examiner stems from hindsight knowledge impermissibly derived from the Appellant's disclosure.

For at least these reasons, the Appellant respectfully asserts that the Examiner has not established a *prima facie* case of obviousness for claim 1. The Appellant submits that the rejection of claim 1 is improper and requests that the rejection of claim 1 be reversed by the honorable Board.

Claims 3-7, 9 and 10

Claims 3-7, 9 and 10 are dependent on and further limit claim 1. Since the rejection of claim 1 is believed improper, the rejection of claims 3-7, 9 and 10 are also believed improper for at least the same reasons as claim 1.

Claim 11

Claim 11 was rejected as allegedly obvious over Kocher in view of Curry and in further view of Ng. FOA, pg. 2. A *prima facie* case for obviousness can only be made if the combined reference documents teach or suggest all the claim limitations. MPEP 2143.

Claim 11 recites, in part, "periodically retrieving CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs." App., claim 11. Claim 11 appears to be rejected under reasoning very similar to claim 1. FOA, pg. 4. Specifically, the Final Office Action indicates that neither Kocher nor Ng teach the preceding limitations, but alleges Curry discloses the claim element at column 2, lines 26-41. FOA, pg. 4-5.

As discussed above, the Appellant respectfully disagrees with the Examiner's interpretation of Curry's teachings. Contrary to the Examiner's assertions, there is no teaching in Curry of periodically retrieving CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, as recited in claim 11. Additionally, the only suggestion for combining Kocher and Curry in the manner advanced by the Examiner stems from hindsight knowledge impermissibly derived from the Appellant's disclosure.

For at least these reasons, the Appellant respectfully asserts that the Examiner has not established a *prima facie* case of obviousness for claim 11. The Appellant submits that the rejection of claim 11 is improper and requests that the rejection of claim 11 be reversed by the honorable Board.

Claims 12-15 and 17

Claims 12-15 and 17 are dependent on and further limit claim 11. Since the rejection of claim 11 is believed improper, the rejection of claims 12-15 and 17 are also believed improper for at least the same reasons as claim 11.

Claim 18

Claim 18 was rejected as allegedly obvious over Kocher in view of Curry and in further view of Ng. FOA, pg. 2. A *prima facie* case for obviousness can only be made if the combined reference documents teach or suggest all the claim limitations. MPEP 2143.

Claim 18 recites, in part, "creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, the retrieval agents configured to periodically retrieve CRLs at time intervals from the different CAs and to consolidate the CRLs from multiple CAs." App., claim 18. The Final Office Action states that claim 18 is rejected on the same grounds as claim 11. FOA, pg. 6.

As discussed above, the Appellant respectfully disagrees with the Examiner's interpretation of Curry's teachings. Contrary to the Examiner's assertions, there is no teaching in Curry of creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, the retrieval agents configured to periodically retrieve CRLs at time intervals from the different CAs and to consolidate the CRLs from multiple CAs, as recited in claim 18. Additionally, the only suggestion for combining Kocher and Curry in the manner advanced by the Examiner stems from hindsight knowledge impermissibly derived from the Appellant's disclosure.

For at least these reasons, the Appellant respectfully asserts that the Examiner has not established a *prima facie* case of obviousness for claim 18. The Appellant submits that the rejection of claim 18 is improper and requests that the rejection of claim 18 be reversed by the honorable Board.

Claims 19-21

Claims 19-21 are dependent on and further limit claim 18. Since the rejection of claim 18 is believed improper, the

rejection of claims 19-21 are also believed improper for at least the same reasons as claim 18.

II. Claims 2, 8 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry and Ng, and further in view of Ginter (US 6,658,568)

Claims 2 and 8

Claims 2 and 8 are dependent on and further limit claim 1. Since the rejection of claim 1 is believed improper, the rejection of claims 2 and 8 are also believed improper for at least the same reasons as claim 1.

Claim 12

Claim 12 is dependent on and further limits claim 11. Since the rejection of claim 11 is believed improper, the rejection of claim 12 is also believed improper for at least the same reasons as claim 11.

III. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry in view of Ng, and further in view of Hassler

Claim 3 is dependent on and further limits claim 1. Since the rejection of claim 1 is believed improper, the rejection of claim 3 is also believed improper for at least the same reasons as claim 1.

IV. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry in view of Ng, and further in view of Kaliski

Claim 5 is dependent on and further limits claim 1. Since the rejection of claim 1 is believed improper, the rejection of claim 5 is also believed improper for at least the same reasons as claim 1.

V. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curry in view of Ng in view of Ginter, and further in view of Strellis

Claim 9 is dependent on and further limits claim 1. Since the rejection of claim 1 is believed improper, the rejection of claim 9 is also believed improper for at least the same reasons as claim 1.

Conclusion

In view of the foregoing, Appellant submits that the rejections of claims 1-15 and 17-21 are improper and respectfully requests that the rejections of claims 1-15 and 17-21 be reversed by the Board.

Respectfully submitted,

Dated: January 31, 2008

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (866) 607-8538

Claims Appendix

Claim 1. A system comprising:

a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and different CAs may use different CRL distribution mechanisms;

multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs;

a plurality of CRL databases for storing the consolidated CRLs from the multiple CRL retrieval agents and/or the replications of CRLs, the CRL databases storing at least one individually identifiable revoked digital certificate; and

a CRL access user interface for providing a uniform set of Application Program Interfaces for users accessing the CRLs in the CRL database, said system enabling consolidation and access of the certificate revocation lists (CRLs) from the plurality of certificate authorities (CAs).

Claim 2. A system according to claim 1, wherein said plurality of CRL databases include a central CRL database and a plurality of CRL replication databases, said central CRL database for storing the consolidated CRLs from the multiple CRL retrieval agents, and said plurality of CRL replication databases for storing the replications of the CRLs of the central CRL database.

Claim 3. A system according to claim 1, wherein said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases.

Claim 4. A system according to claim 1, wherein said plurality of CRL retrieval agents include a HTTP/CRL retrieval agent, for periodically retrieving CRLs from specified HTTP servers and updating the CRL database.

Claim 5. A system according to claim 1, wherein said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for

periodically sending Request For Comments 1424/Certificate-Revocation List retrieval request and receiving CRL retrieval reply.

Claim 6. A system according to claim 1, wherein said plurality of CRL retrieval agents include a Http retrieval agent triggered by a HTTP request, said Http receiver agent verifies an authorization of the requester, if successful, said agent stores each transmitted CRL in the CRL databases.

Claim 7. A system according to claim 1, wherein said plurality of CRL retrieval agents further verifies the integrity and the authenticity of the retrieved CRLs.

Claim 8. A system according to claim 1, wherein a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency.

Claim 9. A system according to claim 2, wherein a hub-and-spoke replication architecture is used among said central CRL database and said plurality of CRL replication databases.

Claim 10. A system according to claim 1, wherein said system is also adapted for consolidating and accessing at least one kind of revoked certificate list.

Claim 11. In a secure network implemented by digital certificates, a method for certificate revocation list (CRL) consolidation and access, wherein a plurality of certificate authorities (CAs) maintain and distribute the digital certificates revoked by themselves in the form of CRLs, and different CAs may use different CRL distribution mechanisms, said method comprising the steps of:

periodically retrieving CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs;

consolidating the CRLs from multiple CAs;

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate; and

accessing the CRLs from the CRL databases by a uniform set of Application Program Interfaces.

Claim 12. A method according to claim 11, said plurality of CRL databases include a central CRL database and a plurality of CRL replication database, said central CRL database for storing the consolidated CRLs from multiple CRL retrieval agents and said plurality of CRL replication database for storing the replications of the CRLs of the central database.

Claim 13. A method according to claim 11, wherein said method is also adapted for consolidation and accessing all kinds of revoked certificate lists.

Claim 14. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11.

Claim 15. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11.

Claim 17. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 11.

Claim 18. A method comprising:

employing a secure network implemented by digital certificates for certificate revocation list (CRL) consolidation and access, with a plurality of certificate authorities (CAs) maintaining and distributing the digital certificates revoked by themselves in the form of CRLs, wherein different CAs may use different CRL

distribution mechanisms, including the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, the retrieval agents configured to periodically retrieve CRLs at time intervals from the different CAs and to consolidate the CRLs from multiple CAs;

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate; and

accessing the CRLs form the CRL databases by a uniform set of Application Program Interfaces.

Claim 19. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 18.

Claim 20. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 18.

Claim 21. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 18.

Evidence Appendix

None.

Related Proceedings Appendix

None.